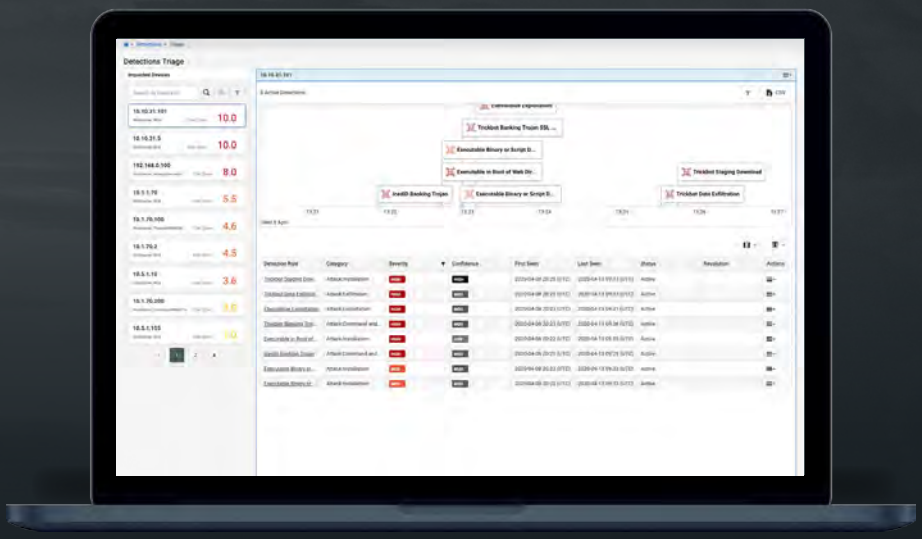
Faster, More Efficient Threat Triage with Gigamon ThreatINSIGHT™

Workflows Increase a Security Teams' Ability to Detect and Respond to Threats

Your network is rapidly changing, and employees, applications and trust zones are more distributed than ever.

Securing a growing number of dispersed devices against increasingly sophisticated and diligent threat actors is a burden on security teams who are inundated with alerts — and have no clear plan for addressing them.



MANUAL TRIAGING COMES AT PRICE

To decrease risk, security professionals must respond quickly and triage alerts accurately, but their efforts are hampered by having little context and having to dig through too many alerts. As a result, response times lag and teams often cannot triage all alerts, allowing potential threats to go unaddressed. ThreatINSIGHT presents findings in a clear and easy to understand timeline and automates the analysis of the findings security teams need to make quick and accurate triage decisions.

THREATINSIGHT DOES THE HEAVY LIFTING — SO YOU CAN FOCUS ON CRITICALLY IMPACTED ASSETS

ThreatINSIGHT detections are derived from a deep understanding of risk, machine-learning detection analytics and threat-management workflows. As such, ThreatINSIGHT offers the context needed for effective prioritization and rapid response.

KEY BENEFITS

+ **See at a glance all compromised devices.** With a few clicks, you can see a list of all devices impacted by a threat.

+ **Know which threats to investigate first.** ThreatINSIGHT instantly prioritizes threats and dynamically calculates the risk of the threat to your organization.

+ **Quickly understand the order of events.** ThreatINSIGHT provides a visual timeline of events that lets you quickly see historical context and severity ratings to speed up mean time to remediation.

+ **Gain additional insight on potential threats.** ThreatINSIGHT analyzes behavioral characteristics of DNS and SSL traffic and provides visibility into potentially emerging threats and provides recommended next steps for remediation.

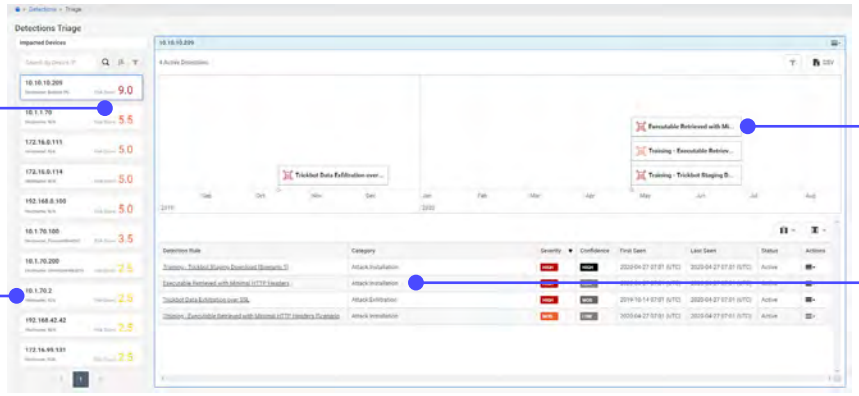
+ **Receive support from a Technical Account Manager.** As part of your subscription, receive help from security experts who are familiar with your needs. They're available to enable your teams, provide security expertise, guidance and analysis of your environment. TAMs provide security guidance and continuity, as well as customized support of your ThreatINSIGHT deployment.

Prioritize Risk

Risk scoring designed to help analysts prioritze detections and determine which activity to triage first.

Device Identification

Analysts can quickly identify impacted assets to reduce time spent on triage.



Time Context

Timeline helps visualize the order of events that occurred on the impacted device.

Correlated Activity

Observe all threat activity associated with the impacted device. Drill-down deeper to gather activity details.

Gauge Severity & Confidence

Quickly understand the activity severity rating and the level of confidence in the detection accuracy.

Detection Details

Full description of threat activity. Steps for investigation and remediation (per Gigamon ATR).

Threat Indicators

Highlight the indicators observed in this detection. Indicators presented with time context.

From Triage to Mitigation, ThreatINSIGHT Does It All

TRIAGE
Answer questions like: 'Is this threat real?', And, 'how do I prioritize it?'

INVESTIGATION
Dig deep to answer "Who, what, when, where and how" and the extent of the incident

CORROBORATION
Validate the findings and assess the severity of a threat

MITIGATION
Automated responses and device remediations through integrations

Gigamon ThreatINSIGHT is the first network detection and response (NDR) solution purpose built to help you secure your rapidly changing, increasingly complex network. It enables you to:

+ Detects suspicious DNS and SSL traffic associated with emerging threats via machine learning
+ Automate risk calculation and incident prioritization, to help teams quickly focus on high priority incidents and riskiest assets for faster response
+ Help teams improve security posture by enumerating out of date protocols and certificates along with early stage threat tactics such as cataloging authentication/authorization privileges
+ Deploy security tools, through zero-touch visibility into new network segments within minutes
+ Track historical threat activity on devices regardless of change, such as asset reimaging
+ Improve investigation workflows, reduce time and effort spent finding relevant details
+ Accelerate threat hunting by isolating key threat behaviors, and change from reactive detection to proactive hunting and mitigation

WHY GIGAMON?

Gigamon enables organizations to run fast, stay secure and innovate in the digital economy by providing complete visibility and intelligence on all data in motion across their hybrid cloud network. The numbers below highlight the Gigamon journey that started in 2004. Since then, we've been awarded over 60 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations around the world.

Take ThreatINSIGHT for a test drive, visit gigamon.com/demo.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com

05.20_01